



QUALYS SECURITY CONFERENCE 2020

The Need to Shift Left and What It Means to Security

Alex Mandernack
Security Solution Architect
Product Management
Qualys, Inc

Traditional World

Each app team
builds their
own image
(CentOS v1, v2,
v3)

Deploy application
(1, 2, 3)

Inefficiencies,
slows things down,
no standardization
across teams,
repetition in
security workflows

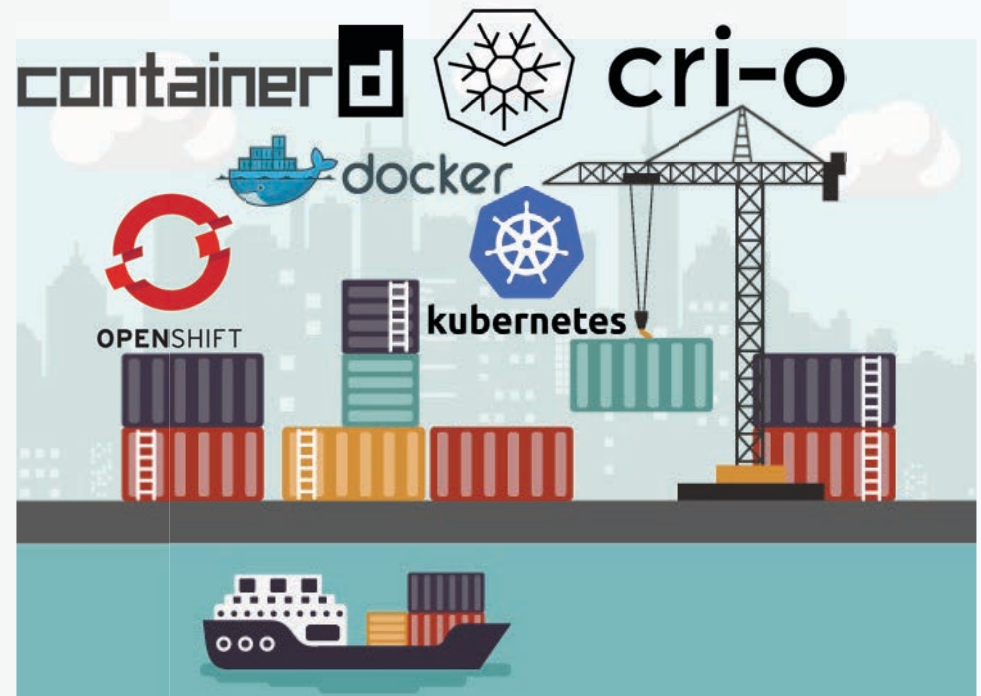
PenTest report to Dev
(t0+1Mo)

- Dev team dealing with out of date findings
- Not machine readable
- Repeated work across apps 1, 2, 3 (OS level vulns)
- Not doing it often enough due to cost, efficient reasons

Scan in production
(VM, WAS, PC etc.)

- Findings for app 1, 2, 3
- Separate patching workflows for running production workloads (v1, v2, v3)

The Driver: Scale, Elasticity & DevOps Pipeline



The background is a solid blue color with a pattern of small white dots arranged in a grid. Three of these dots are highlighted in red, located at approximately (10%, 55%), (15%, 75%), and (85%, 25%) in normalized coordinates. The text is centered in the middle of the image.

Can Security
Teams do
Better?

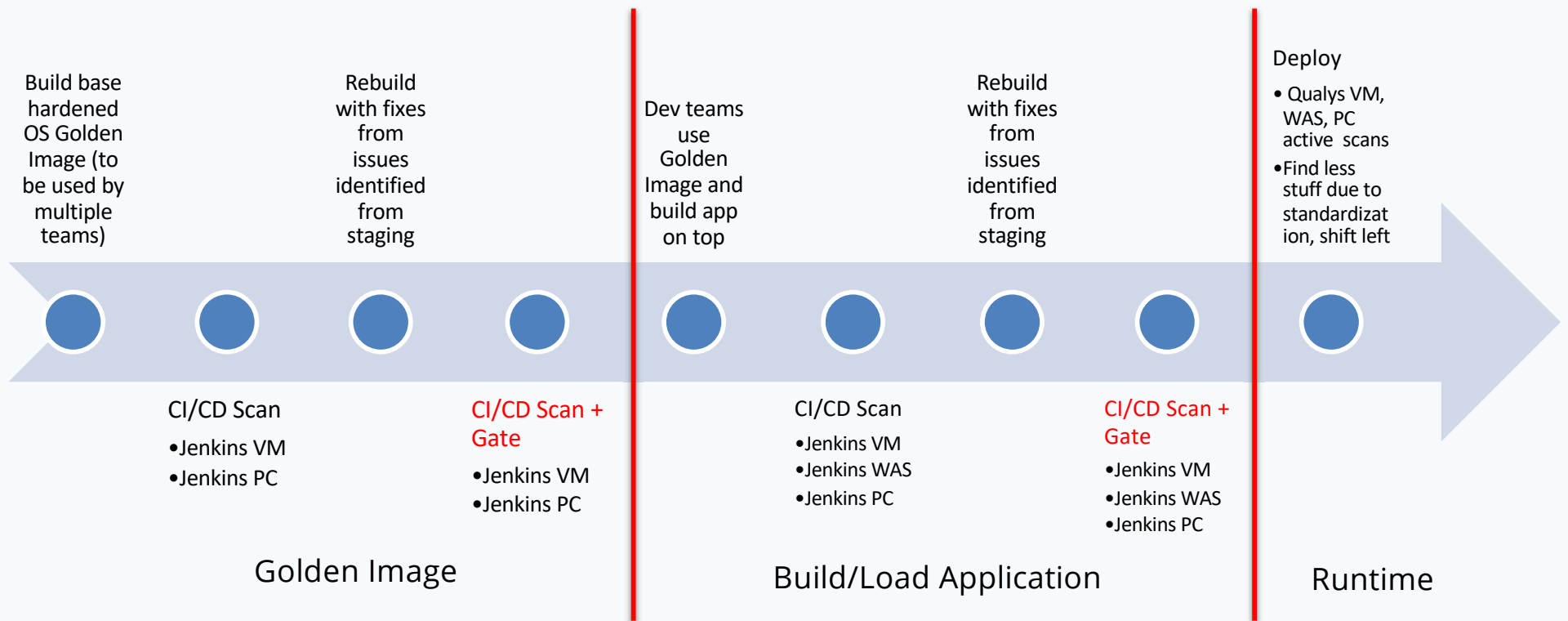
Shifting Security to the Left

- Developers and security teams must think about security, sooner
- Get security tools into the process earlier
- Automate! Leverage API's, CI plugins
- Golden images
- Scan in the CI pipeline
 - Vulnerability gates in the pipeline
 - Vulnerability information at the fingertips of Dev

The New Role of the Security Team

- Must not be a roadblock
- Provide security tooling that is self-service for DevOps, Dev
 - CI Plugins
 - APIs
 - Scripting
- Verify and audit the process
 - Dashboards/live data
 - Trending

Shift Left with Qualys!



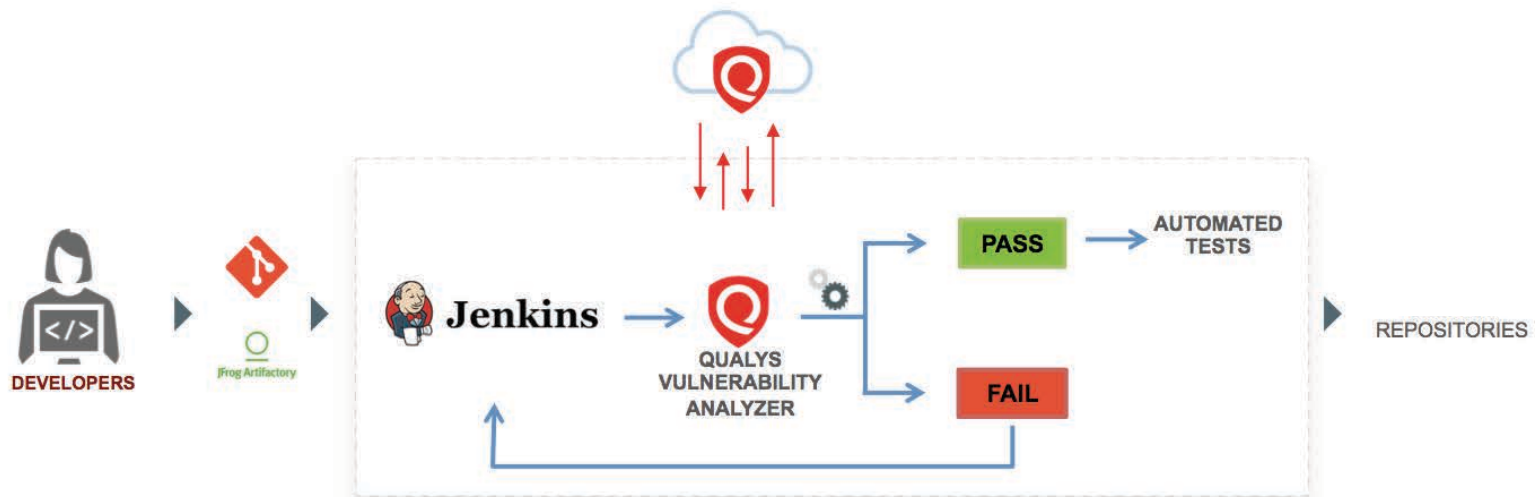
Qualys Jenkins Plugin

Available on the Jenkins Marketplace

- Vulnerability Management
- Container Security
- Web Application Scanning
- API Security



Secure the CI Pipeline



Jenkins Vulnerability Management Plugin

The screenshot displays the Jenkins Vulnerability Management Plugin interface, which integrates with the Qualys Vulnerability Analyzer. The interface is divided into several sections:

- Header:** Jenkins logo, search bar, and user information (admin, log out).
- Left Sidebar:** Contains the Jenkins logo, a search bar, and a list of items (test_pipeline, #4) with a link to the Qualys Report for 10.113.197.71.
- Main Content Area:**
 - Qualys Vulnerability Analyzer Results:** A section showing the scan status (FAILED) and scan name (test_pipeline_jenkins_build_4_2019-05-21-10-18-26).
 - Results Summary:** A summary of the scan results, including the type (API), launch date (05/21/2019 10:18:39), network (Global Default Network), total duration (00:04:09), and scan target (10.113.197.71).
 - Criteria Evaluation:** A table showing the evaluation of criteria (QIDs, CVEs, CVSS) with a red 'X' for QIDs and a green checkmark for CVEs.
 - Vulnerabilities Table:** A table listing vulnerabilities with columns for QID, Title, CVE ID, Severity, CVSSv2 Base Score, CVSSv3 Base Score, Category, PCI Vuln?, Type, and Bug Traq ID. The table shows 13 entries, including vulnerabilities like Hidden RPC Services, TCP Test-Services, OpenSSH Xauth Command Injection Vulnerability, OpenSSH Multiple Vulnerabilities, OpenSSH 7.4 Not Installed Multiple Vulnerabilities, OpenSSH Information Disclosure and Denial of Service Vulnerability, OpenSSH Username Enumeration Vulnerability, SSH Server Public Key Too Small, Deprecated SSH Cryptographic Settings, and OpenSSH LoginGraceTime Denial of Service Vulnerability.

Page generated: May 21, 2019 12:04:45 PM UTC | Jenkins ver. 2.164.2

Jenkins WAS Plugin

Jenkins 5 search GP | log out

Jenkins > WASPluginFreestyle_2 > #23 > Qualys WAS Scan Status

Qualys

Summary

Vulnerabilities

Scan ID: 23011099

Scan Name: WASPluginFreestyle_2_jenkins_build_23_2019-02-14-17-14

Scan Status: **FINISHED**

Scan Reference: was/1550144060224.32559210

Scan Report: [Click here to view Scan Report on Qualys Portal](#)

Target URL: <http://google-gruyere.appspot.com/922324844025/>

Results Summary

Results Status: SUCCESS

Auth Status: Not Used

Number of Requests: 1688

Links Crawled: 12

Total Duration: 18 min 45

Results Stats

Vulnerabilities (43)

Jenkins 5 search GP | log out

Jenkins > WASPluginFreestyle_2 > #23 > Qualys WAS Scan Status

Qualys

Summary

Vulnerabilities

Criteria Evaluation

QUALYS VULNERABILITIES RESULTS


Show 10 entries

QID	Title	URL	Available Unauthenticated?
150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities	http://google-gruyere.appspot.com/922324844025/feed?uid=%22%3E%3Cqss%20a%3DX166455440Y1Z%3E	Yes
150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities	http://google-gruyere.appspot.com/922324844025/login?uid=%3CEMBED%20SRC%3D%2F%2Flocalhost%2Fq.swf%20All%20owScriptAccess%3Dalways%3E%3C%2FEMBED%3E&pw=password	Yes
150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities	http://google-gruyere.appspot.com/922324844025/snippets.gtl?uid=%20onEvent%3DX166495526Y1Z%20	Yes
150053	Login Form is Not Submitted Via HTTPS	http://google-gruyere.appspot.com/922324844025/saveprofile	Yes
150053	Login Form is Not Submitted Via HTTPS	http://google-gruyere.appspot.com/922324844025/login	Yes
150081	X-Frame-Options header is not set	http://google-gruyere.appspot.com/922324844025/feed.gtl?uid=cheddar	Yes
150081	X-Frame-Options header is not set	http://google-gruyere.appspot.com/922324844025/feed.gtl	Yes
150081	X-Frame-Options header is not set	http://google-gruyere.appspot.com/922324844025/#	Yes
150081	X-Frame-Options header is not set	http://google-gruyere.appspot.com/922324844025/	Yes
150081	X-Frame-Options header is not set	http://google-gruyere.appspot.com/922324844025/newaccount.gtl	Yes

Showing 1 to 10 of 43 entries

Previous 1 2 3 4 5 Next


Jenkins Container Security Plugin

 Jenkins

3


search

[Jenkins](#) > [pipeline-project](#) > [#78](#) > [Qualys Report For e8d112ff7588](#)

 Qualys

[Build Summary](#)
[Vulnerabilities](#)
[Installed Software](#)
[Layers](#)

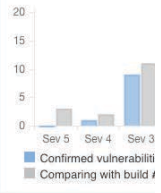
BUILD REPORT - e8d112ff7588




Build Status: Failed
Tags: latest
Image ID: e8d112ff7588
Size: 828 MB

Build Summary

The vulnerabilities count by severity for image id e8d112ff7588 exceeded one of the configured threshold value :
Configured : Severity 1 > 0; Severity 2 > 0; Severity 3 > 0; Severity 4 > 0; Severity 5 > 0;
Found : Severity 1: 0, Severity 2: 1, Severity 3: 11, Severity 4: 2, Severity 5: 0

Vulnerability

Potential Vulner.


Qualys Report For e8d112ff7588[ENABLE AUTO REFRESH](#)

INSTALLED SOFTWARE

Show 10 entries

Search:

Name	Installed Version	Fixed In Version
libmagickwand-dev	8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
libmagickwand-6-headers	8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
libmagickcore-dev	8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
libmagickcore-6-headers	8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
imagemagick-6.q16	8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4





Demo

Qualys GitHub

Automation scripts

Reporting scripts

Open Source
community



<https://github.com/Qualys>



QUALYS SECURITY CONFERENCE 2020

Thank you

Alex Mandernack
amandernack@qualys.com